

AXIS Camera Station S2224 Mk II Appliance

目次

使用に当たって	4
デバイスをインストールする	5
.....	5
設定例	5
独立した監視ネットワークでのセットアップ	5
既存のネットワークでのセットアップ	6
スイッチをコーポレートネットワークに直接接続する	7
デバイスを構成する	9
Axisレコーダーの初期設定	9
サーバーとの接続	9
リモートサーバーとの接続	10
AXISセキュアリモートアクセスにサインイン	10
AXIS Camera Station Proの設定	11
ビデオ管理システムを起動する	11
デバイスの追加	11
録画方法の設定	12
ライブビデオを表示する	12
録画の表示	12
ブックマークの追加	12
録画のエクスポート	12
AXIS File Playerでの録画の再生と検証	13
ネットワーク設定	13
サーバーポートの設定	13
セキュリティに関する考慮事項	14
システムをオンラインでライセンスする	14
オフラインのシステムをライセンスする	14
ローカル Windows® ユーザーアカウントの管理	16
ユーザーアカウントの作成	16
管理者アカウントを作成します。	16
ローカルユーザーグループを作成する	16
ユーザーアカウントを削除します。	16
ユーザーアカウントのパスワードを変更する	17
ユーザーアカウントのパスワードリセットディスクを作成する	17
AXIS Camera Station Proのユーザーアカウントの管理	18
ユーザー権限	18
ユーザーまたはグループの追加	18
ユーザーまたはグループの権限	19
デバイスを管理する	22
セキュアブートの証明書を更新する	22
証明書のステータスを確認する	22
推奨されるアクション	23
BIOSを通じて証明書を更新する	23
Windows Updateを通じて証明書を更新する	23
現在のBIOSのバージョンを確認する	24
BIOSを更新する	24
Windows®を更新します	24
Windows®の更新プログラムの設定を構成する	24
ストレージを追加する	25
ベゼルを取り外します。	25
ハードドライブを取り付ける	26
新しい録画ストレージを追加する	26
RAIDボリュームの作成	27
Microsoft Windows®でRAIDボリュームを初期化する	27

内蔵スイッチの管理.....	28
内蔵スイッチの設定について	28
スイッチの管理ページにログインする.....	28
ランニングコンフィグレーション	28
概要.....	28
電力管理	29
電力の割り当て.....	29
PoEをオン/オフにする.....	31
ネットワークオーバービュー	31
ポートのロックとロック解除.....	32
設定.....	32
ネットワーク設定	32
日付と時刻を設定します。	33
DHCPサーバーの設定	33
SNMP設定	33
メンテナンス	33
ファームウェアの更新.....	33
スイッチを再起動します。	34
スイッチの設定をバックアップする.....	34
スイッチの設定を復元する	34
証明書の管理	34
パスワードの変更	34
Web設定の構成.....	35
工場出荷時の設定にリセットします。	35
ログ.....	35
スイッチ レポートの作成	35
仕様	36
製品概要	36
前面と背面.....	36
LEDインジケーター	36
トラブルシューティング	38
サーバーをリセットする.....	38
システムリカバリの実行.....	38
.....	38
AXIS Camera Station Proのトラブルシューティング	39
さらに支援が必要ですか?.....	40
参考リンク	40
サポートに問い合わせる	40

使用に当たって

AXIS Camera Station Pro録画サーバーを設定する標準的なワークフローは次のとおりです。

1. デバイスをインストールする。
2. Windows®の初期設定:装置を設置した後、いくつかの手順に従って、地域、言語、キーボードレイアウト、管理者アカウントとそのパスワードを設定します。
3. Axisレコーダーの初期設定:Windowsの初期設定の後、AXIS Recorder Toolboxが開き、コンピューター名、日付と時刻、ネットワークなど、基本的かつ必要な設定を行う手順が表示されます。Axisレコーダーの初期設定, on page 9を参照してください。
4. Windows®を構成する.次を行うことをお勧めします。
 - Windows®を最新バージョンに更新します。Windows®を更新します, on page 24を参照してください。
 - 標準ユーザーアカウントを作成します。ユーザーアカウントの作成, on page 16を参照してください。
5. AXIS Camera Station Proを最新バージョンに更新します。
 - システムがオンラインの場合:AXIS Recorder Toolboxアプリを開いて、[**Update AXIS Camera Station Pro (AXIS Camera Station Proの更新)**] をクリックします。
 - システムがオフラインの場合:axis.com に移動し、最新バージョンをダウンロードします。
6. AXIS Camera Station Proクライアントを起動します。
7. AXIS Camera Station Proサーバーに接続します。
8. AXIS Camera Station Proの設定, on page 11.

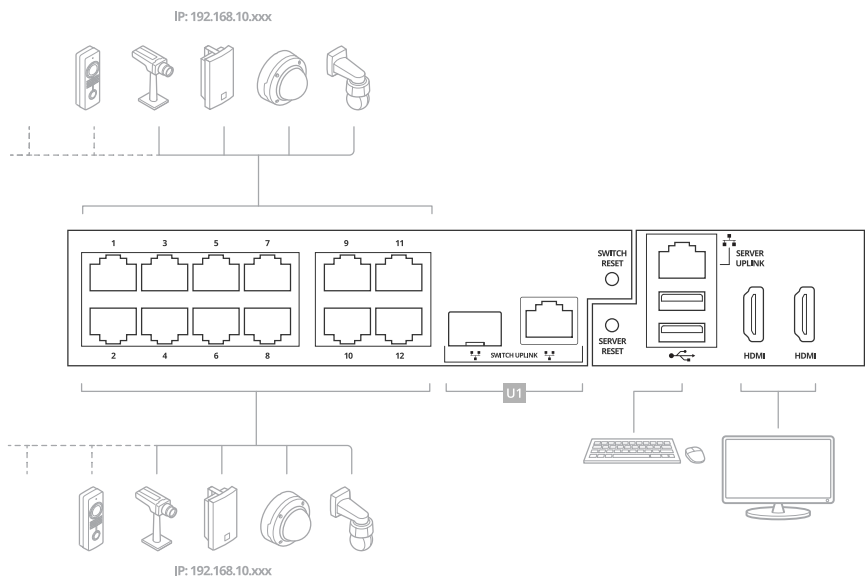
デバイスをインストールする

本製品の設置方法については、同梱されているインストールガイドまたはaxis.comの製品サポートページにあるインストールガイドを参照してください。

設定例

独立した監視ネットワークでのセットアップ

別の外部ネットワークへの相互接続を持たない独立した監視ネットワークを作成できます。このセットアップは、基本的なプラグアンドプレイインストールです。組み込みスイッチのDHCPサーバはデフォルトで有効になっています。カメラをPoEポートに接続するとすぐに、カメラの電源が入り、IPアドレスが取得され、AXIS Camera Station Proからアクセスできるようになります。



難易度	ベーシック
メリット	別の外部ネットワークへの相互接続のない専用監視ネットワーク プラグアンドプレイインストール
制限事項	使用帯域 PoE予算 リモートアクセス不可
必要なアクション	組み込みスイッチのデフォルト パスワードを変更する AXIS Camera Station Proライセンスの登録

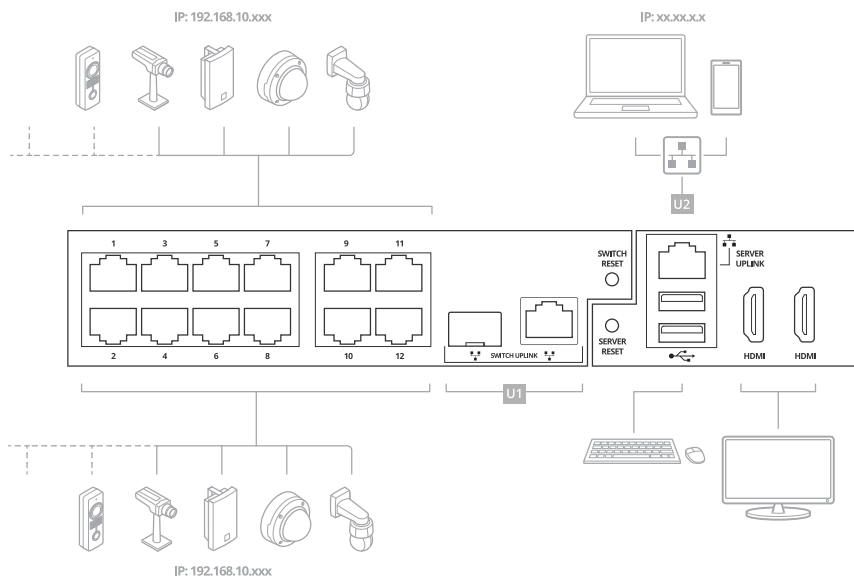
使用するコネクタ	PoEイーサネットポート USB 2.0ポート (キーボードおよびマウス用) Displayport™またはHDMIコネクタ
使用しないコネクタ	スイッチアップリンクポート サーバーアップリンクポート USB 3.2ポート (前面) ユニバーサルオーディオジャック (前面)

既存のネットワークでのセットアップ

既存のネットワーク内に監視ネットワークを作成できます。これは、監視ネットワークが既存のネットワークから分離されていることを意味します。

注

追加のレコーダーを使用する場合、AXIS S30 Recordersなどの機器は録画のためにネットワークデータを監視ネットワークからサーバーネットワークに転送しません。AXIS S30 Recordersがカメラと同じネットワークに接続されていることを確認してください。

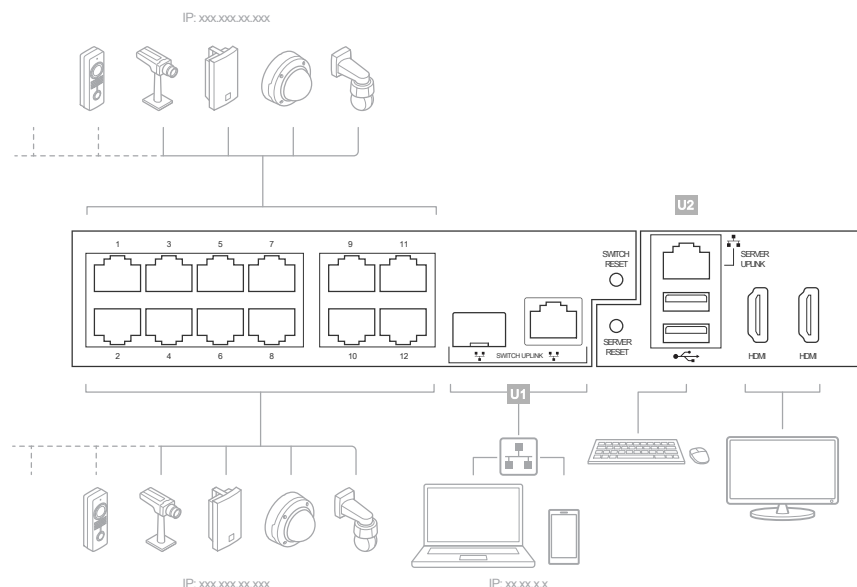


難易度	高度
メリット	AXIS Camera Station Proクライアントを使用して、ネットワーク経由でS22シリーズに接続できる。 ネットワークの分離
制限事項	企業ネットワークポリシーに従う必要がある場合があります。
必要なアクション	組み込みスイッチのデフォルト パスワードを変更する AXIS Camera Station Proライセンスの登録

使用するコネクタ	PoEイーサネットポート イーサネットポート - ネットワーク接続用 サーバーアップリンク (オプションとして) USB 2.0ポート (キーボード およびマウス用) (オプションとして) Displayport™またはHDMI コネクタ
使用しないコネクタ	スイッチアップリンクポート USB 3.2ポート (前面) ユニバーサルオーディオジャック (前面)

スイッチをコーポレートネットワークに直接接続する

この設定により、システムは既存のコーポレートネットワークに直接統合され、ネットワーク上のどこからでもカメラにアクセスして監視できます。



難易度	高度
メリット	カメラはコーポレートネットワークからアクセスでき、SNMPサーバーで監視できます。
制限事項	企業ネットワークポリシーに従う必要がある場合があります。
必要なアクション	スイッチのDHCPをオフにする コーポレートネットワークからスイッチの IP アドレスを静的な IP アドレスに変更する コーポレートネットワーク上で PC の内部 NIC を DHCP または静的 IP に設定する スイッチのデフォルトパスワードを変更します。 AXIS Camera Station Pro の設定と登録

使用するコネクタ	PoEイーサネットポート スイッチアップリンクポート (U1) (オプションとして) USB 2.0ポート (キーボードおよびマウス用) (オプションとして) Displayport™またはHDMIコネクタ
使用しないコネクタ	PCアップリンクポート (U2) USB 3.2ポート (前面) ユニバーサルオーディオジャック (前面)

デバイスを構成する

Axisレコーダーの初期設定

Windows®の設定が完了すると、AXIS Recorder Toolboxが自動的に開き、初回設定のセットアップアシスタントの説明が表示されます。このセットアップアシスタントで、AXIS Recorder Toolboxで装置を管理する前に、いくつかの基本的で必要な設定を行います。

注

設定はサーバー用です。スイッチの設定を変更するには、スイッチの管理ページに移動します。設定, on page 32を参照してください。

1. [Light (ライト)] または [Dark (ダーク)] テーマを選択し、[Next] (次へ) をクリックします (ご使用の製品で選択できる場合)。
2. 必要に応じコンピューター名を変更し、[Next (次へ)] をクリックします。
3. [Date and time (日付と時刻)] で以下の設定を行い、[Next (次へ)] をクリックします。
 - タイムゾーンを選択します。
 - NTPサーバを設定するには、[NTP server (NTP サーバー)] を選択し、NTPサーバーのアドレスを入力します。
 - 手動で設定するには、[Manual (手動)] を選択し、日付と時刻を選択します。
4. [Network settings (ネットワーク設定)] で以下の設定を行い、[Next (次へ)] をクリックします。
 - [Use automatic IP settings (DHCP) (自動IP設定 (DHCP) を使用する)] と [Use automatic DNS settings (自動DNS設定を使用する)] は、デフォルトでオンになっています。
 - デバイスがDHCPサーバーを使用してネットワークに接続されている場合は、割り当てられたIPアドレス、サブネットマスク、ゲートウェイ、および優先DNSが自動的に表示されます。
 - デバイスがネットワークに接続されていないか、利用可能なDHCPサーバーがない場合は、ネットワークの要件に応じて、IPアドレス、サブネットマスク、ゲートウェイ、および優先DNSを手動で入力します。
5. **Finish (終了)** をクリックします。コンピューター名を変更した場合、AXIS Recorder Toolboxからデバイスの再起動を求めるメッセージが表示されます。

サーバーとの接続

AXIS Camera Station S2224 Mk II Applianceクライアントでは、単一のサーバーまたは複数のサーバーに、さまざまな方法で接続することができます。

最後に使用したサーバー - 前のセッションで使用したサーバーに接続します。

このコンピューター - クライアントと同じコンピューターにインストールされているサーバーに接続します。

リモートサーバー - リモートサーバーとの接続, on page 10を参照してください。

注

- サーバーへの初回接続時、クライアントはサーバーの証明書IDを確認します。正しいサーバーに接続していることを確認するには、その証明書IDを AXIS Camera Station S2224 Mk II Appliance Service Controlに表示されているIDと照合します。

Server list (サーバーリスト)	サーバーリストからサーバーに接続するには、 [Server list (サーバーリスト)] ドロップダウンメニューからサーバーを選択します。サーバーリストを作成または編集するには、  をクリックします。
Import server list (サーバーリストのインポート)	AXIS Camera Stationからエクスポートされたサーバーリストファイルをインポートするには、右下の [Import server list (サーバーリストをインポート)] をクリックして、.mslファイルを参照します。
Delete saved passwords (保存したパスワードの削除)	接続されたすべてのサーバーの保存されたユーザー名とパスワードを削除するには、 [Delete saved passwords (保存したパスワードを削除)] をクリックします。
Change client proxy settings (クライアントのプロキシ設定を変更)	サーバーに接続できない場合は、クライアントのプロキシ設定を更新する必要がある場合があります。 [Change client proxy settings (クライアントのプロキシ設定を変更)] をクリックします。

リモートサーバーとの接続

1. **[リモートサーバー]** を選択します。
2. **[Remote server (リモートサーバー)]** ドロップダウンリストからサーバーを選択するか、IPアドレスまたはDNSアドレスを入力します。サーバーが一覧に表示されていない場合は、 をクリックして、利用可能なすべてのリモートサーバーのリストを更新します。サーバーがデフォルトのポート番号 (55754) とは異なるポートでクライアントを受け入れるよう設定されている場合は、IPアドレスの後にポート番号 (192.168.0.5:46001など) を入力します。
3. 以下のいずれかの操作を行います。
 - 現在のWindows® ユーザーとしてログインするには、**[Log in as current user (現在のユーザーでログイン)]** を選択します。
 - **[Log in as current user (現在のユーザーでログイン)]** のチェックマークを外し、**[Log in (ログイン)]** をクリックします。別の認証情報を使用してログインする場合は、**[Other user (その他のユーザー)]** を選択して別のユーザー名とパスワードを入力します。

AXISセキュアリモートアクセスにサインイン

重要

セキュリティと機能性を向上させるため、**Axis セキュアリモートアクセス (v1)** を**Axis セキュアリモートアクセス v2**にアップグレードします。現行バージョンは2025年12月1日をもって提供終了となる予定のため、それまでにAxis Secure Remote Access v2へのアップグレードを強くお勧めします。

お使いの AXIS Camera Station S2224 Mk II Applianceシステムへの影響：

- 2025年12月1日以降、**Axis Secure Remote Access (v1)**を使用してシステムにリモートアクセスすることはできなくなります。
- **Axis セキュアリモートアクセス v2**を使用するには、AXIS Camera Station Pro バージョン 6.8にアップグレードする必要があります。このアップグレードは、2026年3月1日まで、すべてのAXIS Camera Station 5ユーザーを対象に無料で提供されています。

注

- Axis Secure Remote Accessを使用してサーバーに接続しようとする、サーバーはクライアントを自動的にアップグレードできません。
 - プロキシサーバーがネットワークデバイスと AXIS Camera Station S2224 Mk II Appliance サーバーの間にある場合、AXIS Secure Remote Accessを使用してサーバーにアクセスするには、AXIS Camera Station S2224 Mk II Applianceサーバー上のWindowsでプロキシ設定を行う必要があります。
1. [AXISセキュアリモートアクセスにサインイン] リンクをクリックします。
 2. MyAxisアカウントの認証情報を入力します。
 3. [Sign in (サインイン)] をクリックします。
 4. [Grant (許可)] をクリックします。

AXIS Camera Station Proの設定

開始する前に:

- インストール内容に応じてネットワークを設定します。ネットワーク設定を参照してください。
- 必要な場合は、サーバーポートを設定します。サーバーポートの設定を参照してください。
- セキュリティ上の問題を考慮します。セキュリティに関する考慮事項を参照してください。

必要な設定を行ったら、AXIS Camera Station Proで作業を開始ができます。

1. ビデオ管理システムを起動する
2. デバイスの追加
3. 録画方法の設定, on page 12
4. ライブビデオを表示する, on page 12
5. 録画の表示, on page 12
6. ブックマークの追加, on page 12
7. 録画のエクスポート, on page 12
8. AXIS File Playerでの録画の再生と検証, on page 13

ビデオ管理システムを起動する

AXIS Camera Station Proクライアントアイコンをダブルクリックすると、クライアントが起動します。クライアントの初回起動時には、クライアントが同じコンピューターにインストールされたAXIS Camera Station Proサーバーに自動的にログインしようとします。

複数のAXIS Camera Station Proサーバーに、異なる方法で接続できます。

デバイスの追加

AXIS Camera Station S2224 Mk II Applianceを初めて起動すると、[Add devices (デバイスの追加)] ページが開き、デバイスを追加するネットワークを検索します。

1. 追加するデバイスをリストから選択します。デバイスが見つからない場合は、[Manual search (手動検索)] をクリックするか、入力して絞り込みます。
2. [追加] をクリックします。
3. [Close (閉じる)] をクリックして設定をスキップし、後で続行します。ここで設定を続行する場合は以下の手順に従います。

- 3.1. [Quick configuration (クイック設定)] または [Site Designer configuration (Site Designer設定)] を選択します。詳細については、を参照してください。
- 3.2. [Add image overlay for date, time, and text (日付、時刻、テキストの画像オーバーレイを追加する)] を選択して、オーバーレイが設定されていないAxisカメラにオーバーレイを追加します。
- 3.3. [Next (次へ)] をクリックします。
- 3.4. [Recording method (録画方法)] の設定を選択します。
- 3.5. [Next (次へ)] をクリックします。
- 3.6. [Retention time (保存期間)] と [Recording storage (録画ストレージ)] を選択し、[Finish (終了)] をクリックして設定を適用します。

録画方法の設定

1. [設定] - [録画とイベント] - [録画方法] を選択します。
2. カメラを選択します。
3. [Motion detection (動体検知)] または [Continuous (連続)] をオンにします。
4. [適用] をクリックします。

ライブビデオを表示する

1. [Live view (ライブビュー)] タブを開きます。
2. ライブビデオを表示するカメラを選択します。

録画の表示

1. [Recordings (録画)] タブを開きます。
2. 録画を表示するカメラを選択します。

ブックマークの追加

1. 録画に移動します。
2. タイムラインで、ズームインとズームアウトを行い、マーカーが目的の位置になるようにタイムラインを動かします。
3.  をクリックします。
4. ブックマークの名前と説明を入力します。キーワードを使用すると、ブックマークが見つけやすくなります。
5. 録画をロックするには、[録画削除を防止] を選択します。

注

録画のロックを解除するには、[Prevent recording deletion (録画削除を防止)] をクリアするか、ブックマークを削除します。

6. [OK] をクリックして、ブックマークを保存します。

録画のエクスポート

1. [Recordings (録画)] タブを開きます。
2. 録画をエクスポートするカメラを選択します。
3.  をクリックすると、選択マーカーが表示されます。
4. マーカーをドラッグして、エクスポートする録画を含めます。

5.  をクリックして、[Export (エクスポート)] タブを開きます。
6. [Export... (エクスポート...)] をクリックします。

AXIS File Playerでの録画の再生と検証

1. エクスポートした録画を含むフォルダーに移動します。
2. AXIS File Playerをダブルクリックします。
3.  をクリックすると、録画のノートが表示されます。
4. デジタル署名を検証するには、次のようにします。
 - 4.1. [Tools (ツール)] > [Verify digital signature (デジタル署名の検証)] に移動します。
 - 4.2. [Validate with password (パスワードで検証)] を選択し、パスワードを入力します。
 - 4.3. [Verify (検証)] をクリックして検証結果を確認します。

注

- デジタル署名は署名付きビデオとは異なります。署名付きビデオは、そのビデオが録画されたカメラを特定できるため、改ざんされていないことを確認できます。詳細については、署名付きビデオとカメラのユーザーマニュアルを参照してください。
- 保存されたファイルがAXIS Camera Stationデータベースと接続していない場合 (インデックスされていないファイル)、AXIS File Playerで再生できるように変換する必要があります。ファイルの変換については、Axisテクニカルサポートにお問い合わせください。

ネットワーク設定

クライアント、サーバー、接続されているネットワークデバイスが異なるネットワーク上にある場合は、AXIS Camera Station S2224 Mk II Appliance使用する前にプロキシまたはファイアウォールを設定します。

クライアントのプロキシ設定

プロキシサーバーがクライアントとサーバーの間にある場合は、クライアントコンピューターのWindowsでプロキシ設定を行います。詳細については、Axisサポートまでお問い合わせください。

サーバーのプロキシ設定

プロキシサーバーがネットワークデバイスとサーバーの間にある場合は、サーバー上のWindowsでプロキシ設定を行う必要があります。詳細については、Axisサポートまでお問い合わせください。

NATとファイアウォール

クライアントとサーバーがNATまたはファイアウォールで隔てられている場合は、AXIS Camera Station S2224 Mk II Appliance Service Controlで指定されているHTTPポート、TCPポート、ストリーミングポートが、ファイアウォールやNATを通過できるように設定します。ネットワーク管理者にサポートを依頼してください。

サーバーポートの設定

AXIS Camera Station S2224 Mk II Applianceサーバーでは、ポート55752 (HTTP)、55754 (HTTP)、55756 (モバイル通信)、および55757 (モバイルストリーミング) がサーバーとクライアントの間の通信に使用されます。必要な場合、これらのポートはAXIS Camera Station Service Controlで変更できます。

セキュリティに関する考慮事項

カメラおよび録画への不正アクセスを防ぐには:

- すべてのネットワーク装置 (カメラ、ビデオエンコーダ、補助装置) で強力なパスワードを使用します。
- AXIS Camera Station S2224 Mk II Applianceサーバー、カメラ、ビデオエンコーダ、補助デバイスをオフィスネットワークから分離された安全なネットワークにインストールします。AXIS Camera Station S2224 Mk II Applianceクライアントは、インターネットアクセスのあるネットワークなど別のネットワーク上のコンピューターにインストールすることができます。
- すべてのユーザーが強力なパスワードを使用していることを確認してください。

システムをオンラインでライセンスする

自動ライセンスを使用するには、システムを登録し、組織に接続する必要があります。

1. [Configuration (設定)] > [Licenses (ライセンス)] > [Management (管理)] に移動します。
2. [Automatic licensing (自動ライセンス)] がオンになっていることを確認します。
3. [Register... (登録...)] をクリックします。
4. My Axisアカウントを使用してサインインし、画面の指示に従います。
5. [Go to AXIS License Manager (AXIS License Managerに移動)] をクリックして、ライセンスを管理します。詳細については、help.axis.comのMy Systemsユーザーマニュアルをお読みください。

オフラインのシステムをライセンスする

システムを手動でライセンスするには:

1. [Configuration (設定)] > [Licenses (ライセンス)] > [Management (管理)] に移動します。
2. [Automatic licensing (自動ライセンス)] をオフにします。
3. [Export system file... (システムファイルのエクスポート...)] をクリックし、コンピューターにファイルを保存します。

注

AXIS License Managerにアクセスするには、インターネット接続が必要です。クライアントコンピューターにインターネット接続がない場合は、インターネット接続のあるコンピューターにシステムファイルをコピーします。

4. *AXIS License Manager*を開きます。
5. *AXIS License Manager*で:
 - 5.1. 正しい組織を選択するか、まだ作成していない場合は作成します。詳細については、help.axis.comのMy Systemsユーザーマニュアルをお読みください。
 - 5.2. [System setup (システム設定)] に移動します。
 - 5.3. [Upload system file (システムファイルをアップロード)] をクリックします。
 - 5.4. [Upload system file (システムファイルをアップロード)] をクリックし、システムファイルを選択します。
 - 5.5. [Upload system file (システムファイルをアップロード)] をクリックします。
 - 5.6. [Download license file (ライセンスファイルのダウンロード)] をクリックします。
6. AXIS Camera Station S2224 Mk II Applianceクライアントに戻ります。
7. [Import license file... (ライセンスファイルのインポート...)] をクリックし、ライセンスファイルを選択します。

8. [Go to AXIS License Manager (AXIS License Managerに移動)] をクリックして、ライセンスを管理します。

ローカル Windows® ユーザーアカウントの管理

ユーザーアカウントの作成

個人データと情報のセキュリティを強化するために、ローカルアカウントごとにパスワードを追加することをお勧めします。

重要

ローカルアカウントのパスワードを作成したら、そのパスワードを忘れないでください。ローカルアカウントのパスワードを紛失したパスワードを回復する方法はありません。

1. [Settings (設定)] > [Accounts (アカウント)] > [Other users (その他のユーザー)] > [Add other user (その他のユーザーを追加)] の順に移動し、[Add account (アカウントを追加)] をクリックします。
2. [I don't have this person's sign-in information (このユーザーのサインイン情報を持っていない)] をクリックします。
3. [Add a user without a Microsoft account (Microsoftアカウントを持たないユーザーを追加する)] をクリックします。
4. ユーザー名、パスワード、およびパスワードのヒントを入力します。
5. [Next (次へ)] をクリックし、指示に従います。

管理者アカウントを作成します。

1. [Settings (設定)] > [Accounts (アカウント)] > [Other people (その他のユーザー)] に移動します。
2. 変更するアカウントに移動し、[Change account type (アカウントの種類の変更)] をクリックします。
3. [Account type (アカウントの種類)] に移動し、[Administrator (管理者)] を選択します。
4. [OK] をクリックします。
5. デバイスを再起動し、新しい管理者アカウントでログインします。

ローカルユーザーグループを作成する

1. [Computer Management (コンピューター管理)] に移動します。
2. [Local Users and Groups (ローカルユーザーとグループ)] > [Group (グループ)] の順に移動します。
3. [Group (グループ)] を右クリックし、[New Group (新しいグループ)] を選択します。
4. グループ名と説明を入力します。
5. グループメンバーの追加:
 - 5.1. [追加] をクリックします。
 - 5.2. [詳細設定] をクリックします。
 - 5.3. グループに追加するユーザー アカウントを見つけて、[OK] をクリックします。
 - 5.4. もう一度 [OK] をクリックします。
6. [Create (作成)] をクリックします。

ユーザーアカウントを削除します。

重要

アカウントを削除すると、ログイン画面からユーザーアカウントが削除されます。また、ユーザーアカウントに保存されているすべてのファイル、設定、およびプログラムデータも削除します。

1. [Settings (設定)] > [Accounts (アカウント)] > [Other people (その他のユーザー)] に移動します。
2. 削除するアカウントに移動し、[Remove (削除)] をクリックします。

ユーザーアカウントのパスワードを変更する

1. 管理者アカウントでログインします。
2. [User Accounts (ユーザーアカウント)] > [User Accounts (ユーザーアカウント)] > [Manage another account in sequence (別のアカウントを順番に管理する)] の順に移動します。
デバイス上のすべてのユーザーアカウントの一覧が表示されます。
3. パスワードを変更するユーザーアカウントを選択します。
4. [Change the password (パスワードの変更)] をクリックします。
5. 新しいパスワードを入力し、[Change password (パスワードの変更)] をクリックします。

ユーザーアカウントのパスワードリセットディスクを作成する

USBフラッシュドライブにパスワードリセットディスクを作成することをお勧めします。このディスクを使用して、パスワードをリセットできます。パスワードリセットディスクがないと、パスワードをリセットできません。

注

Windows® 10以降を使用している場合は、パスワードを忘れたときのために、ローカルアカウントにセキュリティの質問を追加できるため、パスワードリセットディスクを作成する必要はありません。これを行うには、[Start (スタート)] ボタンをクリックし、[Settings (設定)] > [Sign-in options (サインインオプション)] > [Update your security questions (セキュリティに関する質問の更新)] の順にクリックします。

1. ローカルユーザーアカウントを使用してデバイスにログインします。接続されているアカウントのパスワードリセットディスクを作成することはできません。
2. 空のUSBフラッシュドライブを装置に接続します。
3. [Windows® 検索フィールドから、[Create a password reset disk (パスワード リセット ディスクの作成)] に進みます。
4. パスワードディスクの作成ウィザードで、[Next (次へ)] をクリックします。
5. USBフラッシュドライブを選択し、[Next (次へ)] をクリックします。
6. 現在のパスワードを入力し、[Next (次へ)] をクリックします。
7. 画面の指示に従います。
8. USBフラッシュドライブを取り外し、安全な場所に保管してください。パスワードを何度変更しても、新しいディスクを作成する必要はありません。

AXIS Camera Station Proのユーザーアカウントの管理

ユーザー権限

[Configuration (設定)] > [Security (セキュリティ)] > [User permissions (ユーザー権限)] に移動して、AXIS Camera Station S2224 Mk II Applianceのユーザーとグループを確認します。

注

AXIS Camera Station S2224 Mk II Applianceサーバーを実行しているコンピューターの管理者には、自動的に AXIS Camera Station S2224 Mk II Applianceの管理者権限が付与されます。管理者グループの権限を変更したり、削除したりすることはできません。

ユーザーまたはグループを追加する前に、それらがローカルコンピューターに登録されているか、Windows® Active Directory のユーザーアカウントを持っていることを確認してください。ユーザーまたはグループを追加するには、ユーザーまたはグループの追加を参照してください。

ユーザーがグループに所属している場合、そのユーザーには、個人またはグループに割り当てられる最も高いフォールの権限が付与されます。たとえば、カメラXへのアクセス権を持つユーザーが、カメラYおよびZへのアクセス権を持つグループにも所属している場合、そのユーザーは3つすべてのカメラへのアクセス権を持ちます。

	エントリが1人のユーザーであることを示します。
	エントリがグループであることを示します。
[Name (名前)]:	ローカルコンピューターまたはActive Directoryに表示されるユーザー名。
ドメイン	ユーザーまたはグループが属するドメイン。
役割	ユーザーまたはグループに割り当てられるアクセスロール。表示される値:管理者、オペレーター、閲覧者。
詳細	ローカルコンピューターまたはActive Directoryに表示されるユーザーの詳細情報。
サーバー	ユーザーまたはグループが属するサーバー。

ユーザーまたはグループの追加

Microsoft Windows® とActive Directoryのユーザーとグループは AXIS Camera Station S2224 Mk II Applianceにアクセスできます。ユーザーを AXIS Camera Station S2224 Mk II Applianceに追加するには、ユーザーまたはグループをWindows® に追加する必要があります。

Windows® 10および11でユーザーを追加するには：

- WindowsキーとXを押し、[Computer Management (コンピューターの管理)] を選択します。
- [Computer Management (コンピューターの管理)] の画面で、[Local Users and Groups (ローカルユーザーとグループ)] > [Users (ユーザー)] に移動します。
- [Users (ユーザー)] を右クリックし、[New user (新規ユーザー)] を選択します。
- ポップアップダイアログで、新規ユーザーの詳細を入力し、[User must change password at next login (ユーザーが次回ログオン時にパスワードを変更する必要があります)] をクリアします。
- [Create (作成)] をクリックします。

Active Directoryドメインをご使用の場合は、ネットワーク管理者にお問い合わせください。

ユーザーまたはグループの追加

1. [Configuration > Security > User permissions (設定 > セキュリティ > ユーザー権限)] に移動します。
2. [追加] をクリックします。利用可能なユーザーとグループがリストに表示されます。
3. [Scope (対象)] で、ユーザーとグループを検索する場所を選択します。
4. [Show (表示)] で、ユーザーまたはグループを表示するかどうかを選択します。ユーザーまたはグループが多すぎる場合、検索結果が表示されないことがあります。フィルターを使用して検索結果を絞り込みます。
5. ユーザーまたはグループを選択し、[Add (追加)] をクリックします。

対象	
サーバー	ローカルコンピュータ上のユーザーまたはグループを検索する場合に選択します。
ドメイン	Active Directoryのユーザーまたはグループを検索する場合に選択します。
選択したサーバー	複数の AXIS Camera Station S2224 Mk II Applianceサーバーに接続している場合は、サーバーを選択してそのサーバー上のユーザーまたはグループを検索します。

ユーザーまたはグループの設定

1. リストからユーザーまたはグループを選択します。
2. [Role (権限)] で、[Administrator (管理者)]、[Operator (オペレーター)]、または [Viewer (閲覧者)] を選択します。
3. [Operator (オペレーター)] または [Viewer (閲覧者)] を選択した場合は、ユーザーまたはグループの権限を設定することができます。ユーザーまたはグループの権限を参照してください。
4. [Save (保存)] をクリックします。

ユーザーまたはグループの削除

1. ユーザーまたはグループを選択します。
2. [削除] をクリックします。
3. ポップアップダイアログで [OK] をクリックするとユーザーまたはグループが削除されます。

ユーザーまたはグループの権限

ユーザーまたはグループに割り当てられるロールは3種類です。ユーザーまたはグループの権限の定義方法については、ユーザーまたはグループの追加を参照してください。

管理者 - すべてのカメラのビューのライブおよび録画ビデオへのアクセス、すべてのI/Oポートへのアクセスなど、システム全体へのフルアクセス。このロールは、システム設定にアクセスすることが求められます。

オペレーター - カメラ、ビュー、I/Oポートを選択して、ライブおよび録画ビデオにアクセスします。オペレーターは AXIS Camera Station S2224 Mk II Applianceのすべての機能 (システムの設定を除く) へのフルアクセスが許可されます。

閲覧者 - 選択したカメラ、I/Oポート、ビューのライブビデオにアクセスします。録画ビデオへのアクセスやシステムの設定を行うことはできません。

カメラ

[Operator (オペレーター)] または [Viewer (閲覧者)] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。

アクセス	カメラおよびすべてのカメラ機能へのアクセスを許可します。
ビデオ	このカメラからのライブ映像へのアクセスを許可します。
音声を聞く	カメラから受話するアクセスを許可します。
音声送話	カメラに送話するアクセスを許可します。
Manual Recording (手動録画)	手動で録画を開始・停止することができます。
Mechanical PTZ (メカニカルPTZ)	メカニカルPTZコントロールへのアクセスを許可します。メカニカルPTZを搭載したカメラでのみ使用できます。
PTZ優先度	PTZ優先度を設定します。数値が小さいほど、優先度が高いことを意味します。優先度を割り当てない場合は [0] に設定されます。優先度が最も高いのは管理者です。優先度の高い権限を持つユーザーがPTZカメラを操作する場合、デフォルトでは、他のユーザーは同じカメラを10秒間操作することができません。メカニカルPTZを搭載したカメラで、[Mechanical PTZ (メカニカルPTZ)] が選択されている場合のみ使用できます。

ビュー

[Operator (オペレーター)] または [Viewer (閲覧者)] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。複数のビューを選択し、アクセス権を設定することができます。

アクセス	AXIS Camera Station S2224 Mk II Applianceのビューへのアクセスを許可します。
編集	AXIS Camera Station S2224 Mk II Applianceで表示を編集することができます。

I/O

[Operator (オペレーター)] または [Viewer (閲覧者)] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。

アクセス	I/Oポートへのフルアクセス権を許可します。
読む	I/Oポートの状態を変更せずに確認することができます。
Write (書き込み)	I/Oポートの状態を変更することができます。

システム

リスト内でグレー表示されているアクセス権限は設定できません。チェックマークは、そのユーザーまたはグループがこの権限を持っていることを意味します。

[Operator (オペレーター)] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[Take snapshots (スナップショットを撮る)] は [Viewer (閲覧者)] 権限でも利用できます。

スナップショットを撮る	ライブビューおよび録画モードでスナップショットを撮影することができます。
録画のエクスポート	録画のエクスポートを許可します。
インシデントレポートの生成	インシデントレポートの生成を許可します。
Prevent access to recordings older than (これより古い録画へのアクセスを防止)	指定した分数よりも古い録画へのアクセスを防止します。ユーザーはこれらの録画を検索しても見つけることができません。
アラーム、タスク、ログへのアクセス	アラーム通知を受け取り、[Alarms and tasks (アラームとタスク)] バーと [Logs (ログ)] タブへのアクセスを許可します。
Access data search (データ検索へのアクセス)	イベント発生時の状況を追跡するためのデータ検索を許可します。
イベントにカテゴリーを追加する	録画 タブでイベントにカテゴリーを追加できるようにします。
イベントからカテゴリーを削除する	録画タブでイベントからカテゴリーを削除できるようにします。

アクセスコントロール

[Operator (オペレーター)] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[Access Management (アクセス管理)] は [Viewer (閲覧者)] 権限でも利用できます。

アクセスコントロールの設定	ドアとゾーン、識別プロファイル、カードフォーマットとPIN、暗号化通信、マルチサーバーを設定することができます。
アクセス管理	アクセス管理ができます。また、Active Directory設定にアクセスすることができます。

Viewer (閲覧者) のロールを持つユーザーまたはグループは、次のアクセス権を利用できます。

システムのヘルスマニタリング

[Operator (オペレーター)] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[>システムの健全性監視へのアクセス] は [Viewer (閲覧者)] 権限でも利用できます。

システムの健全性監視の設定	システムの健全性監視を設定することができます。
システムの健全性監視へのアクセス	システムの健全性監視にアクセスすることができます。

デバイスを管理する

セキュアブートの証明書を更新する

Microsoftは2011年に発行されたセキュアブート証明書の提供を2026年6月に終了し、新しい2023年の証明書に切り替えます。レコーダーを安全に保つため、有効期限までに2023年の証明書をインストールしてください。

2023年の証明書のインストールには、Windows 10 LTSC (Long-Term Servicing Channel) または Windows 11 LTSCが必要です。お使いのデバイスが保証期間内であるにもかかわらず、LTSCバージョンではなくWindows 10 SAC (Semi-Annual Channel) が動作している場合は、Axis Technical Supportにお問い合わせください。BIOSの更新や証明書の変更を行う前に、LTSCバージョンにアップグレード可能かどうかをお知らせします。

注

2026年6月以降、2023年の証明書を持たないデバイスは、引き続き通常通り動作しますが、Windows Boot Managerの更新や新たな脆弱性に対する失効リストなど、初期ブートプロセスに対する新しいセキュリティ保護は提供されません。

証明書のステータスを確認する

以下の方法で、2023年の証明書がインストールされており、Windowsのブートローダーが更新されていることを確認します。

方法1:

1. [Registry Editor (レジストリエディタ)] を開きます。
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicingに移動します。
3. UEFICA2023Statusの値を確認します。値が「Updated (更新済み)」となっている場合、2023年の証明書がインストールされています。

ab (Default)	REG_SZ	(value not set)
ab BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
ab ConfidenceLevel	REG_SZ	No Data Observed - Action Required
oi ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
oi LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
ab UEFICA2023Status	REG_SZ	Updated
oi WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

方法2:

1. [Windows Security (Windowsセキュリティ)] を選択します。
2. [Device security (デバイスセキュリティ)] に移動します。
3. [Secure boot (セキュアブート)] で、ステータスメッセージを確認します。証明書が最新の状態であれば、カードには、"Secure Boot is on and all required certificate updates have been applied.No further certificate changes are needed." (セキュアブートはオンです。必要なすべての証明書の更新は適用されています。証明書の変更は必要ありません。) と表示されます。

Secure boot

Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

注

Windowsセキュリティは、デバイスに2026年4月14日付けの累積更新プログラム以降がインストールされている場合のみ、証明書のステータスを表示します。証明書の状態に関するメッセージが表示されない場合は、最新のWindows更新プログラムをインストールするか、代わりに方法1をお試しください。

推奨されるアクション

BIOSの更新により、2023年の証明書がファームウェアに永続的に保存されます。これが最も信頼性の高い方法であるため、Windows Updateを通じてすでに証明書をインストール済みの場合もこの方法をお勧めします。

重要

Windows Updateを通じて証明書をインストールしただけでは、その後、BIOSのセキュアブートキーを工場出荷時の設定にリセットすると、証明書が失われ、セキュアブートがオンになっている状態ではデバイスが起動しなくなります。セキュアブートキーをリセットする前に、BIOSを更新して証明書を永続化してください。

BIOSを通じて証明書を更新する

使用しているモデルに対応するBIOSバージョン、またはそれ以降のバージョンをインストールしてください。これらは、Axis.comの製品ページからダウンロードできます。

モデル	BIOSの最低バージョン
AXIS S2208	TBC
AXIS S2212	TBC
AXIS S2216	TBC
AXIS S2224	TBC
AXIS S2108	Z218-004
AXIS S2208 Mk II	Z670-005
AXIS S2212 Mk II	Z671-005
AXIS S2216 Mk II	Z672-005
AXIS S2224 Mk II	Z673-005

Windows Updateを通じて証明書を更新する

使用しているモデルでBIOSアップデートがまだ提供されていない場合は、代わりにWindows Updateを通じて2023年の証明書を入手することができます。

重要

この方法でインストールされた証明書は、ファームウェアではなく、現在のセキュアブートデータベースに保存されます。BIOSのセキュアブートキーを工場出荷時の設定にリセットすると、証明書が失われ、セキュアブートがオンになっている状態ではデバイスが起動できなくなる可能性があります。この方法をすでに使用している場合も、モデルのBIOSアップデートが利用可能になり次第、インストールしてください。

以下のパスに従って使用します。

1. 使用しているデバイスがWindows 10 LTSCまたはWindows 11 LTSCを実行していることを確認します。
2. 2026年4月14日以降にリリースされたすべてのWindows更新プログラムをインストールします。

3. [Windows Security (Windowsセキュリティ)] > [Device security (デバイスセキュリティ)] > [Secure Boot (セキュアブート)] に移動して、証明書のステータスを確認します。
4. 最新のアップデートをインストールしても証明書が更新されない場合は、レジストリ値 **UEFICA2023Status**を確認します。使用しているデバイスで自動アップデートができない場合は、BIOSを更新するか、Axis Technical Supportにお問い合わせください。

重要

使用環境のすべてのリカバリメディア、ブート環境、およびドライバーが2023年の証明書によって署名されていることを確認するまでは、2011年の証明書を手動で取り消さないでください。その前に2011年の証明書を取り消すと、セキュアブートがオンになっている状態でデバイスを起動できなくなります。

現在のBIOSのバージョンを確認する

現在のBIOSを確認するには:

1. デバイスの電源を入れ、Axisロゴが表示されるまでDELキーを繰り返し押します。
2. [Main (メイン)] の最初の項目として、バージョン番号が表示されます。

BIOSを更新する

BIOSファイルのダウンロードページに掲載されているBIOSガイドに記載されている手順に従ってください。

Windows®を更新します

Windows®は定期的に更新プログラムをチェックします。更新プログラムが利用可能になると、デバイスは自動的に更新プログラムをダウンロードしますが、インストールは手動で行う必要があります。

注

スケジュールされたシステムの再起動中に録画が中断されます。

更新プログラムを手動で確認するには、次の手順を実行します。

1. [Settings (設定)] > [Windows Update (Windows更新プログラム)] に移動します。
2. [Check for updates (クリックして更新)] をクリックします。

Windows®の更新プログラムの設定を構成する

必要に応じて、Windows®の更新プログラムを実行する方法とタイミングを変更できます。

注

スケジュールされたシステムの再起動中に、進行中のすべての録画が停止します。

1. 実行アプリを開きます。
 - [Windows System (Windowsシステム)] > [Run (実行)] に移動するか、
2. gpedit.mscと入力し、[OK] をクリックします。ローカルグループポリシーエディタが開きます。
3. [Computer Configuration (コンピューターの構成)] > [Administrative Templates (管理用テンプレート)] > [Windows Components (Windowsコンポーネント)] > [Windows Update (Windows更新プログラム)] の順に移動します。
4. 必要に応じて設定を構成します (例を参照)。

例:

ユーザーの操作なしで更新プログラムを自動的にダウンロードしてインストールし、必要に応じて営業時間外に装置を再起動するには、次の設定を使用します。

1. [Always automatically restart at the scheduled time (常にスケジュールされた時刻に自動的に再起動する)] を開き、次のいずれかを選択します。
 - 1.1. 有効
 - 1.2. 再起動タイマーにより、ユーザーは作業を保存する次の時間の猶予が得られます (分):15.
 - 1.3. [OK]をクリックします。
2. [Configure Automatic Updates (自動更新の構成)] を開き、次の項目を選択します。
 - 2.1. 有効
 - 2.2. Configure Automatic updates (自動更新を構成する):自動ダウンロードとインストールのスケジュール設定
 - 2.3. Schedule Install day (インストール日のスケジュール):毎週日曜日
 - 2.4. Schedule Install time (インストール時刻のスケジュール):00:00
 - 2.5. [OK]をクリックします。
3. [Allow Automatic Updates immediate installation (自動更新を直ちにインストールする)] を開き、次を選択します。
 - 3.1. 有効
 - 3.2. [OK]をクリックします。

ストレージを追加する

ストレージの要件が合わないことがあります。多くの場合、保存されたデータに保持期間が設定されている場合や高解像度の録画を保存する場合は、追加のストレージをインストールする必要性が発生します。このセクションには、AXIS S22シリーズ製品に追加のハードディスクドライブを設置する方法が説明されています。

注

以下の手順に従って、AXIS S22製品にストレージを追加してください。この手順は現状有姿で提供されています。この手順の実行中にデータや設定が失われた場合もAxis Communications ABは責任を負わないものとします。標準的な対策を講じて、ビジネス上重要なデータをバックアップしてください。次のストレージ拡張手順は、Axisの技術サポートでは対応していません。

注

静電気放電を避けるため、内部システムコンポーネントの作業中は常に静電気マットと静電気ストラップを使用することをお勧めします。

保証

保証の詳細については、www.axis.com/support/warrantyを参照してください。



このビデオを見るには、このドキュメントのWebバージョンにアクセスしてください。

ベゼルを取り外します。

1. ベゼルの両側にある2つのつまみネジを緩めます。
2. ベゼルを取り外します。

ハードドライブを取り付ける

▲ 注意

- AXIS S22シリーズでの使用がテストおよび承認されたハードドライブのみを使用してください。
 - ハードドライブをインストールするときは、ハードドライブキャリアが奥まで押し込まれていることを確認してください。ドライブキャリアがロックされるとカチッと音がします。
 - ハードドライブを取り付ける前に、電源コードが抜かれていることを確認してください。
1. システムをシャットダウンし、電源がオフになっていることを確認してください。
 2. 電源コードを抜きます。
 3. ハードドライブキャリアの前面にあるリリースボタンを押し、ハードドライブキャリアのハンドルを開きます。
 4. ハンドルを使ってハードドライブキャリアを引き出します。
 5. ハードドライブをハードドライブキャリアに取り付けます。
 6. 4本のネジでハードドライブをハードドライブキャリアに固定します。
 7. ハードドライブキャリアがバックプレーンと接続されるまで、キャリアをハードドライブスロットに挿入します。
 8. ハードドライブキャリアのハンドルを閉じて、ハードドライブを所定の位置にロックします。
 9. フロントベゼルを再び取り付けます。
 10. システムを起動します。

新しい録画ストレージを追加する

1. Windowsで新規ハードディスクパーティションを作成してフォーマットします。
 - 1.1. [Start (スタート)] メニューを右クリックし、[Disk Management] (ディスクの管理) を選択します。
 - 1.2. [Initialize Disk (ディスクの初期化)] のポップアップが表示されたら、[OK] をクリックします。表示されない場合は、新しいハードディスクドライブを右クリックし、[Initialize Disk (ディスクの初期化)] を選択します。
 - 1.3. 初期化されたハードディスク上の割り当てられていない領域を右クリックし、[New Simple Volume (新しいシンプルボリューム)] を選択します。
 - 1.4. ウィザードに従ってボリュームサイズを設定し、ドライブレターを割り当てて、パーティションをフォーマットします。
 - 1.5. ウィザードを完了し、新しいシンプルボリュームを作成します。
2. AXIS Camera Station Proに新しい録画ストレージを追加する:
 - 2.1. AXIS Camera Station Proを開きます。
 - 2.2. [Storage (ストレージ)] > [Management (管理)] に移動します。
 - 2.3. [Add... (追加...)] をクリックします。
 - 2.4. 新しく追加したドライブを選択し、[OK] をクリックします。
 - 2.5. [Storage (ストレージ)] > [Selection (選択)] に移動します。
 - 2.6. 録画データを新しいドライブに転送するデバイスを選択します。
 - 2.7. [Store to (保存先)] のドロップダウンリストで新しいドライブを選択し、[Apply (適用)] をクリックします。

ストレージ管理の詳細については、AXIS Camera Station Pro - ユーザーマニュアルを参照してください。

RAIDボリュームの作成

1. RAIDボリュームで使用するディスクが検知されていることを確認してください。
 - 1.1. デバイスをオンにした直後にAxisロゴが表示されるまで素早くF12キーを押します。
 - 1.2. UEFIブートメニューで、**[Device Configuration (装置設定)]** を選択し、Enterを押します。
 - 1.3. Intel® Rapid Storage Technologyメニューで、**[Non-RAID Physical Disks (非RAID物理ディスク)]** にディスクが正しく表示されていることを確認します。

注

物理的に追加ドライブ1台分のスペースしかない装置で利用できるのは、RAID 0とRAID 1のみです。

2. Intel Rapid Storage Technologyメニューで、**[Create RAID Volume (RAIDボリュームの作成)]** を選択し、Enterを押します。
3. ボリュームの名前を入力します。
4. RAIDレベルを選択します。
 - 4.1. **[RAID Level (RAIDレベル)]** を選択し、Enterを押します。
 - 4.2. ポップアップダイアログで、使用するRAIDレベルを選択し、enterを押します。
5. ボリュームで使用するディスクを含めます。
 - 5.1. ディスクを選択し、enterを押します。
 - 5.2. ☒ を選択すると、このディスクがボリュームに含まれます。
 - 5.3. 使用するすべてのディスクを選択するまで、この手順を繰り返します。
6. 特に指定がない限り、**[Stripe Size (ストライプサイズ)]** と **[Capacity (容量)]** はデフォルト値のままにします。
7. **[Create Volume (ボリュームの作成)]** を選択し、enterを押します。
8. Intel Rapid Storage Technologyメニューの **[RAID Volumes (RAIDボリューム)]** に、新しく作成されたRAIDボリュームが表示されます。
9. Escキーを押し、Yキーを押して保存し、UEFIメニューを終了します。
10. CTRL + ALT + DELETEキーを押して、装置を再起動します。

Microsoft Windows®でRAIDボリュームを初期化する

新しいボリュームを設定するには:

1. **[Start (スタート)]** メニューを右クリックし、**[Disk Management] (ディスクの管理)]** を選択します。
2. ポップアップされる **[Initialize Disk (ディスクの初期化)]** で、**[GPT]** を選択し、**[OK]** をクリックします。
3. 未割り当てのディスクを右クリックし、**[New Simple Volume (新しいシンプルボリューム)]** を選択します。
 - セットアップアシスタントの手順に従います。
4. セットアップアシスタントが完了すると、**[Disk Management (ディスクの管理)]** に新しいボリュームが表示されます。**[Disk Management (ディスクの管理)]** を閉じると、システムによって新しいボリュームが使用されるようになります。

内蔵スイッチの管理

内蔵スイッチの設定について

AXIS Camera Station S22 Mk II Appliance Series は、内蔵パワーオーバーイーサネット (PoE) スイッチが付属しています。組み込みスイッチを設定および管理できます。

スイッチの目的は、スイッチによって管理されるセキュリティカメラと関連トラフィック (PoE およびスイッチアップリンクポート) が他のネットワークと共有されないように、ネットワーク上のトラフィックを分離することです。

スイッチの電源管理は、次の規則に従います。

- 各ポートは、接続されている受電デバイスのPoEクラスに従って電力を確保できます。手動でポートに電力を割り当てることもできます。
- 特定のポートの実際の消費電力がそのポート用に確保された電力を上回ると、そのポートはシャットダウンされます。
- すべてのポートの実際の消費電力が電源から供給可能な合計電力量を上回った場合は、ポートはシャットダウンされます。ポートのシャットダウンの順序は、ポートの優先度に従います (小さいポート番号ほど優先度は高くなります)。

スイッチの管理ページにログインする

1. メニューバーに移動します。
 - Webブラウザから、スイッチのIPアドレスを入力します。デフォルト:192.168.10.1
 - AXIS Recorder Toolboxから、[Switch > Open the switch configuration (スイッチ > スイッチの設定を開く)] の順に移動します。
2. ユーザー名とパスワードでログインします。
 - ユーザー名はadminです。
 - パスワードはユニット上部に貼付されているステッカーまたは箱に同梱されている自己接着式のステッカーに表示されています。

メニューバーからログアウトし、スイッチの管理ページを終了します。

ランニングコンフィグレーション

ランニングコンフィグレーションとは、ネットワークデバイスで現在アクティブで動作している設定です。デバイスの現在の状態や機能をリアルタイムで反映します。ただし、デバイスを再起動すると、これらの変更は保存されません。

対照的に、スタートアップコンフィグレーションは、デバイスの不揮発性メモリーに保存される設定一式です。この設定は、デバイスの起動時または再起動時にロードされ、適用されます。

Webインターフェースで変更を行い、[Save (保存)] をクリックすると、その変更が実行中の設定に適用されます。

設定をスタートアップコンフィグレーションに保存するには、Webインターフェースの右上の保存アイコンを使用します。

実行中の設定に未保存の変更がある場合、アイコンが黄色で点滅します。

概要

メニューバーで、[Overview (オーバービュー)] をクリックします。

総合案内

カテゴリー	アイテム	説明
ポートの概要	アクティブなポート	使用中のポート数。
	PoEを使用しているポート	使用中のPoE対応のポート数。
	ロックされたポート	ロックされたポート数。
電力消費量	現在のPoE電力使用量	デバイスが消費するPoE電力のワット数と、専用PoE電力の合計のうち、消費されたPoE電力の割合。
	要求される電力	デバイスに割り当てられた合計電力 (ワット数と割合)。
ポートステータス	アクティブ	ポートは使用中です。
	非アクティブ	ポートを使用する準備ができました。
	ブロック	ポートがブロックされています。

注

ポートをクリックすると、そのポートの詳細情報を表示できます。

電力管理

メニューバーで、[Power management (電源管理)] をクリックします。

ポートリスト

アイテム	説明
ポート	デバイスが接続されているポート番号です。
PoE	PoEステータスです。アイコンをクリックすると、ポートのPoEをオンまたはオフにできます。
PoE class	接続されたデバイスのPoEクラスです。
優先度	接続されたデバイスへの電源割り当ての優先度。デフォルトでは、優先順位はポート番号です。
消費電力 (W)	ポートに接続されているデバイスが消費する電力 (ワット単位)。
要求される電力 (W)	ポートに接続されているデバイスに必要な電力 (ワット単位)。
割り当てられた電力 (W)	ポートに割り当てられた電力を手動で調整します。 電源割り当て方法として [Manual (手動)] を選択した場合にのみ使用できます。

電力の割り当て

PoE電源は、次の方法で接続されているデバイスに割り当てることができます。

- **PoE Class:** スイッチは、接続された装置のPoE Classに基づいてPoE電力を割り当てます。
- **手動:** 接続されているデバイスに割り当てられたPoE電源を手動で調整できます。

- **LLDP-MED:**スイッチは接続されたデバイスと通信し、必要に応じてPoE電源を動的に割り当てます。

注

LLDP-MEDの電源割り当て方式は、AXIS OS 9.20以降のカメラのみで機能します。

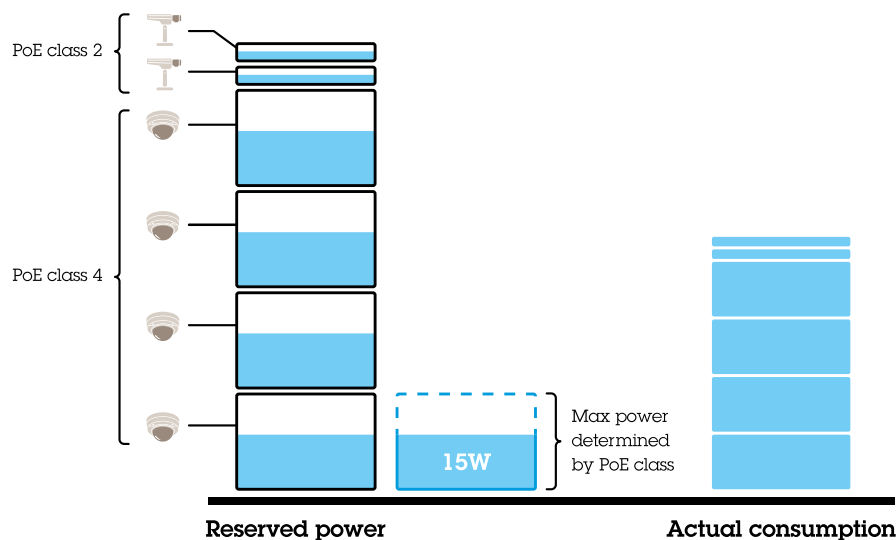
電力配分方法を変更するには、次の手順に進みます。

1. スwitchの電源管理ページで、**[Power management (電源管理)]** に移動します。
2. **[PoE Class]**、**[Manual (手動)]**、または **[LLDP-MED]** を **[Allocate power (電力の割り当て)]** で選択します。
3. **[Manual (手動)]** を選択した場合は、**[Power allocated (電源割り当て)]** の列で、接続したデバイスに割り当てる電源を変更できます。
4. 接続されているデバイスの優先度を変更する場合は、そのデバイスの優先度を選択します。他のデバイスの優先順位は自動的に変更されます。

例:

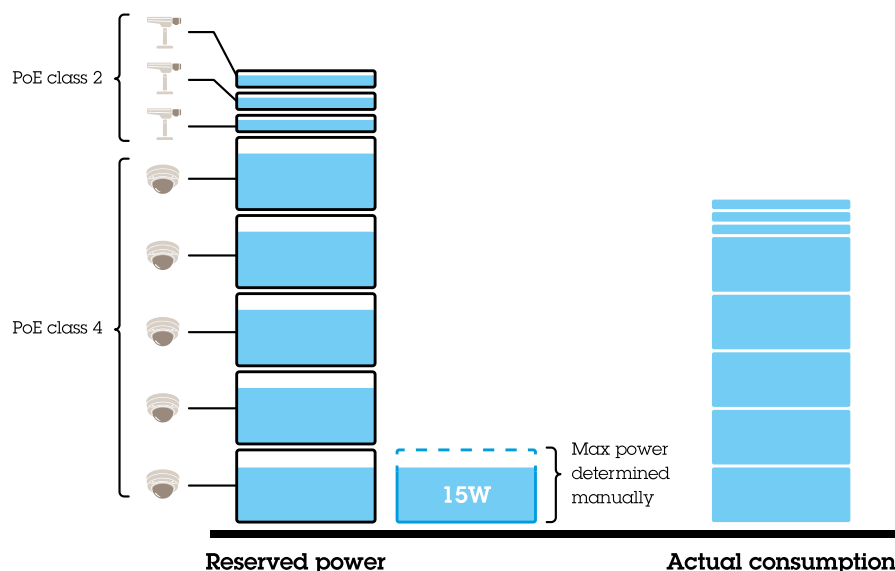
この例では、スイッチの総電力容量は135 Wです。PoE Class 4のデバイスは30 Wの電力を要求しますが、消費電力は15Wのみです。PoE Class 2のデバイスは7 Wの電力を要求しますが、消費電力は5 Wのみです。

PoE Classによる電力の割り当て



各デバイスによって要求される電力は、PoE Classによって決まります。スイッチは、4つのPoE Class4デバイスと2つのPoE Class2デバイスに電力を供給できます。要求される合計電力は $(4 \times 30) + (2 \times 7) = 134$ Wです。実際の消費電力は $(4 \times 15) + (2 \times 5) = 70$ Wです。このようにして、接続されているすべてのデバイスに十分な電力が保証され、優先順位はそれほど重要ではありません。

手動で電力を割り当てる



要求された電力は、PoE Class4デバイスの場合には手動で20 Wに調整されます。スイッチは、5つのPoE Class4デバイスと3つのPoE Class2デバイスに電力を供給できます。要求される合計電力は $(5 \times 20) + (3 \times 7) = 121 \text{ W}$ です。実際の消費電力は $(5 \times 15) + (3 \times 5) = 90 \text{ W}$ です。このようにして、接続されているすべてのデバイスに十分な電力が保証され、優先順位はそれほど重要ではありません。

PoEをオン/オフにする

ポートでPoEをオンにする

1. メニューバーで、**[Overview (オーバービュー)]** をクリックします。
2. [PoE] 列で、 をクリックし、特定のポートでPoEをオンにします。

ポートでPoEをオフにする

1. メニューバーで、**[Overview (オーバービュー)]** をクリックします。
2. [PoE] 列で、 をクリックし、特定のポートでPoEをオフにします。

すべてのポートのPoEをオン/オフにする

1. メニューバーで、**[Power management (電源管理)]** をクリックします。
2. すべてのポートでPoEをオフにするには、**[PoE ports state (PoEポートの状態)]** のドロップダウンメニューに移動し、**[Turn off all (すべてオフ)]** を選択します。
3. すべてのポートでPoEをオンにするには、**[PoE ports state (PoEポートの状態)]** のドロップダウンメニューに移動し、**[Turn on all (すべてオン)]** を選択します。

ネットワークオーバービュー

ネットワークオーバービューは、各ポートのネットワークトラフィックのステータスに関する詳細情報を提供します。

PoEポート

アイテム	説明
ポート	デバイスが接続されているポート番号です。
デバイス	ポートに接続されているデバイスの名前。
IPアドレス	ポートに接続されているデバイスのIPアドレス。

MACアドレス	ポートに接続されているデバイスのMACアドレス。
受信	ポート上の受信データの現在のデータレート (メガビット/秒)。
送信	ポート上の送信データの現在のデータレート (メガビット/秒)。
送信されたパケット	スイッチがネットワークに送信したデータパケット数。
受信されたパケット	スイッチがネットワークから受信したデータパケット数。
失われたパケット	ネットワークの問題により宛先に到達できなかったデータパケットの数と割合。
ロック	ポートがロックされているかどうかを表示します。アイコンをクリックすると、ポートをロックまたはロック解除できます。

ポートのロックとロック解除

MACアドレスをポートにロックすると、そのMACアドレスからのトラフィックだけが渡されるようになります。これによってセキュリティが向上し、権限のないユーザーがセキュリティネットワークにノートPCやその他のデバイスを接続できなくなります。

MACアドレスをポートにロックする

1. メニューバーで、**[Network overview (ネットワークオーバービュー)]** をクリックします。
2. **[Lock (ロック)]** の列で、 をクリックして特定のポートをロックします。

MACアドレスをポートからアンロックする

1. メニューバーで、**[Network overview (ネットワークオーバービュー)]** をクリックします。
2. **[Lock (ロック)]** の列で、 をクリックして特定のポートをアンロックします。

すべてのポートをロックまたはアンロックする

1. メニューバーで、**[Network overview (ネットワークオーバービュー)]** をクリックします。
2. すべてのポートをロックするには、**[Lock ports (ポートをロック)]** のドロップダウンメニューに移動し、**[Lock all (すべてロック)]** を選択します。
3. すべてのポートをアンロックするには、**[Lock ports (ポートをロック)]** のドロップダウンメニューに移動し、**[Unlock all (すべてアンロック)]** を選択します。

設定

ネットワーク設定

スイッチのIPアドレスを変更できます。ただし、ほとんどのカメラのインストールでは、既定の設定を使用することをお勧めします。その理由は、監視ネットワークは通常、企業LANなどの他のネットワークから分離されているためです。この場合、監視ネットワークを使用して、サーバーにインストールされているビデオ管理ソフトウェアから監視デバイスとデータを管理および収集するだけです。

1. メニューバーで、**[Settings (設定)]** > **[Network settings (ネットワーク設定)]** に移動します。
2. 接続の種類、IPアドレス、サブネットマスク、ゲートウェイ、プライマリDNS、セカンダリDNS、およびホスト名を入力します。

注

工場出荷時の設定は次の通りです:アドレス192.168.10.1を持つ静的IP接続と、アドレス255.255.255.0を持つサブネット マスク。

3. **[Save (保存)]** をクリックします。

日付と時刻を設定します。

1. メニューバーで、**[Settings (設定)] > [Date and time (日付と時刻)]** に移動します。
2. 国とタイムゾーンを選択します。
3. 時間を手動で設定するには、**[手動]** を選択し、手動で時間を調整します。
4. NTPサーバを設定するには、**[NTP server (NTP サーバー)]** を選択し、NTPサーバーのアドレスを入力します。

注

NTPは、スイッチがネットワークに接続され、インターネット アクセスで構成されている場合にのみ機能します。

5. **[Save (保存)]** をクリックします。

DHCPサーバーの設定

接続されているデバイスにIPアドレスを割り当てるために内部DHCPサーバを使用するようにスイッチを設定できます。スイッチアップリンク接続を使用して、デバイスが外部アプリケーションにアクセスする、またはアクセスされることを許可する場合は、ゲートウェイとDNSアドレスを指定する必要があります。

1. メニューバーで、**[Settings (設定)] > [DHCP server (DHCPサーバー)]** に移動します。
2. **[Enable DHCP server (DHCPサーバーを有効にする)]** を選択します。
3. 開始IPアドレス、終了IPアドレス、サブネット マスク、ゲートウェイ、プライマリDNS、セカンダリDNS、リースの期間、およびドメイン名を入力します。
4. **[Save (保存)]** をクリックします。

SNMP設定

1. メニューバーで、**[Settings (設定)] > [SNMP]** に移動します。
2. SNMP接続に使用するサーバー名、連絡先、および場所を入力します。
3. SNMPV1またはSNMPV2cを使用する場合は、**[SNMPV1/SNMPV2c]** を選択し、読み取りコミュニティに入ります。
4. SNMPV3を使用する場合は、**[SNMPV3 (MD5)]** を選択し、ユーザ名とパスワードを入力します。

注

現時点では、SNMPに使用されるMD5認証のみをサポートしています。

5. **[Save (保存)]** をクリックします。

メンテナンス

ファームウェアの更新

1. メニューバーで、**[Maintenance (メンテナンス)] > [Update firmware (ファームウェアの更新)]** に移動します。
2. ファームウェア ファイルをドラッグアンドドロップするか、**[Browse (参照)]** をクリックしてファームウェア ファイルに移動します。
3. **[Upload (アップロード)]** をクリックします。

4. ファームウェアの更新が完了したら、スイッチを再起動します。

スイッチを再起動します。

重要

スイッチの再起動中、接続されているすべてのデバイスは、PoEを含むスイッチとの接続を一時的に失います。

1. メニューバーで、**[Maintenance (メンテナンス)]** > **[Reboot switch (スイッチの再起動)]** に移動します。
2. **[Reboot (再起動)]** をクリックし、**[Yes (はい)]** をクリックします。
3. 数分後にスイッチが再起動したら、ログインするためのユーザ名とパスワードを入力します。

スイッチの設定をバックアップする

注

ユーザ名とパスワードはバックアップ ファイルに含まれます。

1. メニューバーで、**[Maintenance (メンテナンス)]** > **[Backup and restore (バックアップと復元)]** に移動します。
2. **[Create a backup file (バックアップ ファイルの作成)]** をクリックします。これにより、.bin形式のバックアップファイルが作成され、**[Downloads (ダウンロード)]** フォルダに保存されます。

スイッチの設定を復元する

注

スイッチの設定を復元するには、バックアップ ファイルを作成しておく必要があります。

1. メニューバーで、**[Maintenance (メンテナンス)]** > **[Backup and restore (バックアップと復元)]** に移動します。
2. バックアップ ファイルをドラッグアンドドロップするか、**[Browse (参照)]** をクリックしてバックアップ ファイルに移動します。
3. **[Upload (アップロード)]** をクリックします。

バックアップファイルからスイッチを再起動するまで数分かかる場合があります。設定が復元されるとスイッチは自動的に再起動するため、再ログインが必要になります。

証明書の管理

1. メニューバーで、**[Maintenance (メンテナンス)]** > **[Manage certificates (証明書の管理)]** に移動します。
2.  をクリックして、秘密キーファイルに移動します。
3.  をクリックして、証明書ファイルに移動します。
4.  をクリックして、CAバンドルファイルに移動します。
5. **[Save (保存)]** をクリックします。
6. スwitchを再起動します。

パスワードの変更

スイッチのデフォルトパスワードを、自分で選択したパスワードに変更できます。

重要

覚えられるパスワードを選択するようにしてください。パスワードを忘れた場合は、工場出荷時の設定にリセットします。、on page 35 を参照して、工場出荷時のパスワードを復元してください。

1. メニューバーで、**[Maintenance (メンテナンス)] > [Change password (パスワードの変更)]** に移動します。
2. 必要に応じて、現在のパスワードと新しいパスワードを入力します。
3. **[Save (保存)]** をクリックします。

Web設定の構成

1. メニューバーで、**[Maintenance (メンテナンス)] > [Web settings (Web設定)]** に移動します。
2. ポート番号を入力します。

注

- ポート番号を変更する場合は、新しいポート番号を書き留めるようにしてください。新しいポート番号を忘れた場合は、工場出荷時の設定にリセットします。、on page 35 を参照して、工場出荷時のポート番号を復元してください。
- HTTPSを有効にしておくことをお勧めします。

工場出荷時の設定にリセットします。

リセットボタンを5秒間押し続けると、スイッチが工場出荷時の設定にリセットされます。

Webインターフェースからスイッチをリセットすることもできます。

1. メニューバーで、**[Maintenance (メンテナンス)] > [Reset to factory (工場出荷時の設定にリセット)]** に移動します。
2. **[Reset (リセット)]** をクリックし、**[Yes (はい)]** をクリックします。

リセットが完了すると、スイッチは自動的に再起動します。

ログ

メニューバーで、**[Logs (ログ)]** をクリックすると、ログのリストが表示されます。列のタイトルをクリックすると、アルファベット順に並べ替えられます。

アイテム	説明
日時	ログイベントが発生した日時。
重大度	警告アイコンとして表示される重大度。
ユーザー	ログイベントを開始したユーザー。
IPアドレス	ログイベントを開始したユーザーのIPアドレス。
サービス	ログイベントが関連付けられているサービス。可能な値は、デスクトップ、ネットワーク、ネットワーク、システム、ntpd、ストレージ、dhcp などです。
イベント	ログイベントの説明。

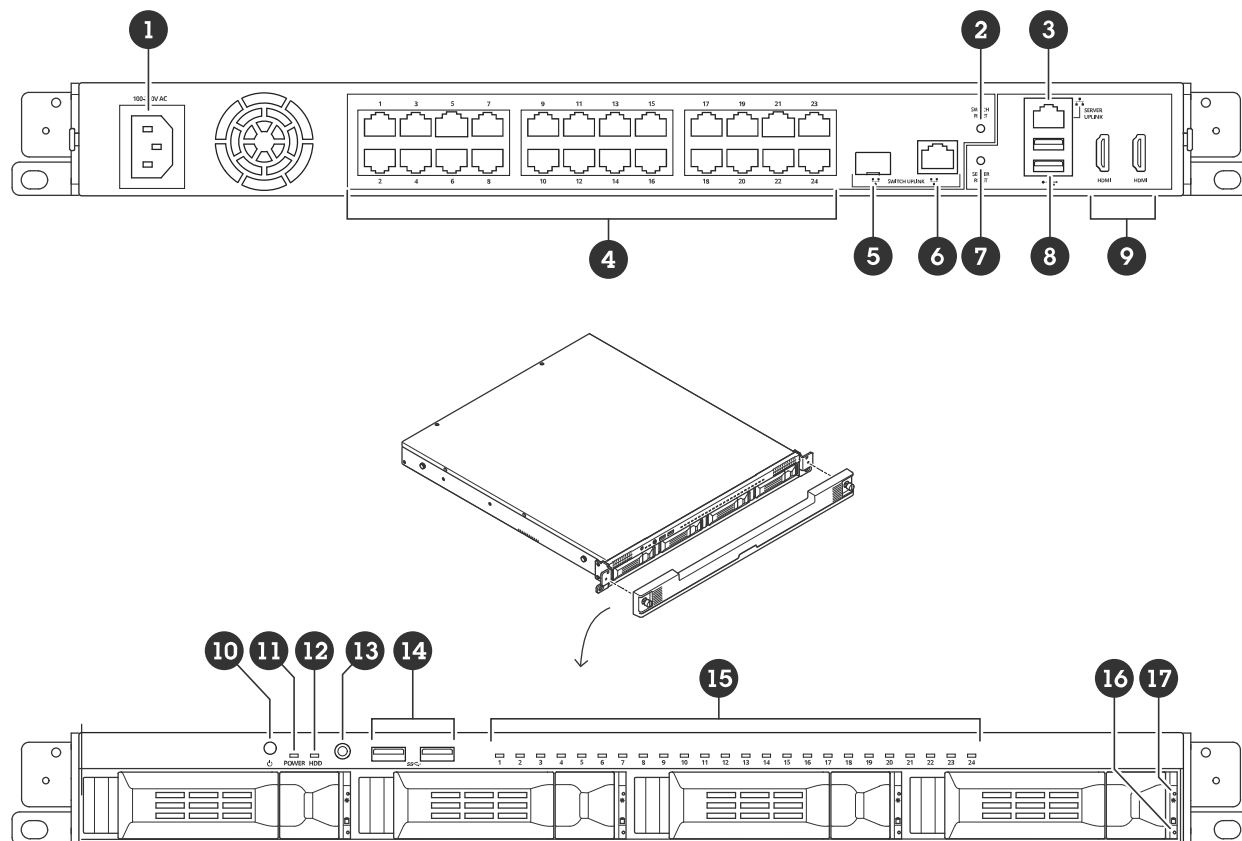
スイッチ レポートの作成

ログページで、**[Export (エクスポート)]** をクリックして、ログページのログエントリを含むスイッチ情報のテキストファイルを作成します。

仕様

製品概要

前面と背面



- 1 電源コネクタ
- 2 スイッチのリセットボタン
- 3 1 GbEイーサネットポート — サーバーアップリンク
- 4 1 GbE PoEイーサネットポート
- 5 1 GbEイーサネットポート — スイッチアップリンク (SFP)
- 6 1 GbEイーサネットポート — スイッチアップリンク (RJ45)
- 7 サーバーのリセットボタン
- 8 USB 2.0ポート
- 9 HDMI™ポート
- 10 電源ボタン
- 11 電源LED
- 12 ハードドライブアクティビティLED
- 13 ユニバーサルオーディオジャック
- 14 USB 3.2ポート
- 15 PoEイーサネットポートのステータスLED
- 16 ハードドライブアクティビティLED
- 17 ハードドライブステータス LED

LEDインジケータ

フロントLED

電源ボタン	電源LED	説明
押していない	オフ	PCとスイッチがオフ
	黄色	PCはオン、スイッチはオフ
	黄点滅	PCはオン、スイッチは起動中
	緑	PCはオン、スイッチ起動完了
押した	0秒まで	スイッチとPCがオフになった場合、両方に電力を送る
	黄点滅するまで (3秒)	スイッチがグレースフルシャットダウンを開始
	赤点滅するまで (6秒)	PCとスイッチがグレースフルシャットダウンを開始
	赤点灯するまで (9秒)	PCがアングレースフルシャットダウンを開始、スイッチがグレースフルシャットダウンを開始

LEDインジケーター	カラー	説明
ハードドライブ (HDD)	緑点滅	ハードドライブのアクティビティ
	赤	考えられるハードドライブの障害
PoEイーサネットポートのステータス	緑	Link State (リンク状態)
	黄色	受電側デバイス、リンクなし状態
	赤	PoE割当量超過
ハードドライブステータス	緑	ハードドライブあり
	赤	考えられるハードドライブの障害

リアLED

ネットワークの速度とアクティビティ	カラー	説明
右LED	黄色	10/100 Mbit/秒
	緑	1000 Mbit/秒
左LED	緑	PoE接続OK
	赤	PoE割当量超過

トラブルシューティング

サーバーをリセットする

サーバーのリセット ボタンを使用して、サーバーをリセットできます。サーバーのリセットには1時間以上かかります。

1. デバイスの電源を切ります。
2. サーバーのリセットボタンを5秒間押し続けます。Windows® REが起動します。
3. [Troubleshoot (トラブルシューティング)] を選択します。
4. [Reset your PC (PCのリセット)] を選択します。
5. [Keep my files (ファイルを保持する)]または[Remove everything (すべて削除)] を選択します。[Keep my files (ファイルを保持する)] を選択した場合は、管理者の資格情報を指定する必要があります。
6. 画面上の指示に従ってください。
7. サーバーが再起動し、Windows® を工場出荷時の設定にリセットする手順が開始されます。



サーバーを工場出荷時の既定の設定にリセットする

システムリカバリの実行

デバイスで完全なシステム障害が発生した場合は、回復イメージを使用してWindows® システムを再作成する必要があります。AXIS Network Video Recorder Recovery Kitをダウンロードするには、Axisの技術サポートに連絡し、お使いの装置のシリアル番号を知らせてください。

注

AXIS Network Video Recorder Recovery Kitには、以下の2つのバージョンがあります。

- **sb11** — 2011年の証明書を使用しているデバイス向けです。
- **sb23** — 2023年の証明書に移行したデバイス向けです。

Recovery Kitをダウンロードする前に、証明書のステータスを確認し、それに応じたバージョンを選択してください。間違ったバージョンを選択すると、インストール後に起動できる結果が生成されず、正しい画像で最初からやり直す必要があります。これによってデバイスが損傷することはありません。

デバイスにすでに2023年の証明書がインストールされている場合、2011年の証明書を手動で失効していない限り、sb11バージョンは引き続き安全に使用できます。失効すると、sb23のみが機能します。

システムを再作成するには:

1. AXIS Network Video Recorder Recovery KitとAXIS Network Video Recorder Recovery:ISO to USB Toolをダウンロードします。
2. USBドライブをコンピューターに挿入します。
 - 16 GBのUSBドライブを使用します。
 - USBドライブがフォーマットされ、既存のデータはすべて消去されます。
3. AXIS Network Video Recorder Recovery:ISO to USB Toolを実行し、画面の指示に従います。USBドライブへのデータの書き込みには約10～15分かかります。

4. AXIS Network Video Recorder Recovery:ISO to USB Toolが完了したら、USBドライブを取り出してデバイスに接続します。
5. デバイスを起動します。
6. Axisのフラッシュ画面が表示されたら、F12キーを押します。
7. **[UEFI: USB Drive (UEFI : USBドライブ)]** をクリックします。
8. USBドライブに移動し、Enterキーを押します。システムがAXIS Network Video Recorder Recovery Kitで起動します。
9. **[Reinstall Operating System (オペレーティングシステムの再インストール)]** をクリックします。
リカバリが完了するまでに約10～15分かかります。詳細な手順については、回復キットのダウンロードを参照してください。

AXIS Camera Station Proのトラブルシューティング

AXIS Camera Station Proのトラブルシューティング方法については、*AXIS Camera Station Pro*ユーザーマニュアルを参照してください。

さらに支援が必要ですか？

参考リンク

- *AXIS Camera Station Pro* ユーザーマニュアル
- *AXIS* セキュアリモートアクセスにサインイン
- *Axis Secure Remote Access v2* にサインインする
- *AXIS Camera Station* のウイルス対策許可リストに含める内容

サポートに問い合わせる

さらにサポートが必要な場合は、axis.com/support にアクセスしてください。

T10207039_ja

2026-09 (M5.2)

© 2024 – 2026 Axis Communications AB